UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

34415 7590 06/15/2009

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2437	

DATE MAILED: 06/15/2009

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/612,198	07/01/2003	Carey Nachenberg	20423-07775	4107

TITLE OF INVENTION: REAL-TIME TRAINING FOR A COMPUTER CODE INTRUSION DETECTION SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	09/15/2009

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

34415 7590 06/15/2009

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/612,198	07/01/2003	Carey Nachenberg	20423-07775	4107

TITLE OF INVENTION: REAL-TIME TRAINING FOR A COMPUTER CODE INTRUSION DETECTION SYSTEM

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$0	$0	$1510	09/15/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
DAVIS, ZACHARY A	2437	726-023000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 ____________________

2 ____________________

3 ____________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. The following fee(s) are submitted:

□ Issue Fee

□ Publication Fee (No small entity discount permitted)

□ Advance Order - # of Copies ____________

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

□ A check is enclosed.

□ Payment by credit card. Form PTO-2038 is attached.

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number ________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

□ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

□ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ____________________ Date ____________________

Typed or printed name ____________________ Registration No. ____________________

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/612,198	07/01/2003	Carey Nachenberg	20423-07775	4107

34415 7590 06/15/2009

SYMANTEC/ FENWICK
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2437	

DATE MAILED: 06/15/2009

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 827 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 827 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Notice of Allowability	**Application No.** 10/612,198	**Applicant(s)** NACHENBERG ET AL.	
	Examiner Zachary A. Davis	**Art Unit** 2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the notice of panel decision from pre-appeal brief review mailed 01 April 2009*.

2. ☒ The allowed claim(s) is/are *1,3,4,6-11,13-16,18-20,22,24 and 25*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) □ All b) □ Some* c) □ None of the:

   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

   1) □ hereto or 2) □ to Paper No./Mail Date _____.

   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

EXAMINER'S AMENDMENT

1. As noted in the advisory action mailed 14 November 2008, the amendment under 37 CFR 1.116 filed after final rejection on 27 October 2008 has been entered. By this amendment, Claim 21 was canceled. No claims were added or amended. Claims 1, 3, 4, 6-11, 13-16, 18-20, and 22-24 are currently pending in the present application.

2. As noted in the notice of panel decision mailed 01 April 2009, in view of the pre-appeal brief request for review filed on 10 December 2008, prosecution in the present application has been reopened.

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Brian Hoffman on 03 June 2009.

4. The application has been amended as follows:

IN THE CLAIMS:

Please **REPLACE** the claims with the following **amended listing of claims**:

1. (Currently Amended) A computer-implemented method for training a database intrusion detection system in real time, said method comprising the steps of:

observing, in real time, commands that are accessing the database during a training phase;

establishing categories responsive to the observed commands;

grouping the commands into the categories;

performing a statistical analysis of the categories, the analysis comprising determining whether a predetermined threshold number of categories has been exceeded;

deriving from said commands, in real time, a set of acceptable commands; and

ending the training phase responsive to a determination that the predetermined threshold number of categories has been exceeded ~~the statistical analysis~~.

2. (Canceled)

3. (Previously Presented) The method of claim 1 wherein the commands are SQL commands.

4. (Previously Presented) The method of claim 1 wherein at least one observed command is selected from the group of commands consisting of a query, an add, a delete, and a modify.

5. (Canceled)

6. (Previously Presented) The method of claim 1 wherein the categories comprise at least one category selected from the group of categories consisting of:

canonicalized commands;

dates and times at which commands access the computer code;
logins of users that issue commands;
identities of users that issue commands;
departments of users that issue commands;
applications that issue commands;
IP addresses of issuing users;
frequency of issuing commands by users;
identities of users accessing a given field within the database;
times of day that a given user accesses a given field within the database;
fields accessed by commands;
combinations of fields accessed by commands;
tables within the database accessed by commands; and
combinations of tables within the database accessed by commands.

7. (Previously Presented) The method of claim 1 wherein:
the categories comprise canonicalized commands; and
each category is a command stripped of literal field data.

8. (Original) The method of claim 1 wherein the observing step comprises at least one of:
real-time auditing; and
in-line interception.

9. (Currently Amended) The method of claim 8 wherein the observing step comprises real-time auditing; and at least one of the following is used to extract the commands for observation:
an API that accesses the database;
code injection;
patching; and
direct database integration.

10. (Currently Amended) The method of claim 8 wherein the observing step comprises in-line interception; and at least one of the following is interposed between senders of the commands and the database:

a proxy;
a firewall; and
a sniffer.

11. (Previously Presented) The method of claim 1 wherein:

during the deriving step, a suspicious activity is tracked; and
subsequent to the deriving step, the suspicious activity is reported to a system administrator.

12. (Canceled)

13. (Previously Presented) The method of claim 1 further comprising, subsequent to the deriving step, an operational phase in which commands that are accessing the database are compared against the set of acceptable commands.

14. (Previously Presented) The method of claim 13 wherein a command that is accessing the database during the operational phase that does not match a command in the set of acceptable commands is flagged as suspicious.

15. (Previously presented) The method of claim 14 wherein, when a command is flagged as suspicious, at least one of the following is performed:

an alert is sent to a system administrator;
the command is not allowed to access the database;
the command is allowed to access the database, but the access is limited;
the command is augmented;
a sender of the command is investigated.

16. (Currently Amended) A computer-readable storage medium containing computer program instructions for training a database intrusion detection system in real time, said computer program instructions performing the steps of:

observing, in real time, commands that are accessing the database during a training phase;

establishing categories responsive to the observed commands;

grouping the commands into the categories;

performing a statistical analysis of the categories, the analysis comprising determining whether a predetermined threshold number of categories has been exceeded;

deriving from said commands, in real time, a set of acceptable commands; and

ending the training phase responsive to a determination that the predetermined threshold number of categories has been exceeded ~~the statistical analysis~~.

17. (Canceled)

18. (Previously Presented) The computer-readable storage medium of claim 16 wherein:

the categories comprise canonicalized commands; and

each category is a command stripped of literal field data.

19. (Previously Presented) The computer-readable storage medium of claim 16 further comprising, subsequent to the deriving step, an operational phase in which commands that are accessing the database are compared against the set of acceptable commands.

20. (Currently Amended) A computer-readable storage medium storing computer executable program code for training a database intrusion detection system in real time, the computer-executable code comprising:

a training module adapted for observing, in real time, commands that are accessing the database during a training phase, establishing categories responsive to the observed commands, grouping the commands into the categories, performing a statistical analysis of the categories to determine whether a predetermined ~~frequency~~ threshold number of ~~for establishing the~~ categories has been exceeded, deriving from the commands, in real time, a set of acceptable commands, and ending the training phase responsive to a determination that the predetermined ~~frequency~~ threshold number has been exceeded; and

coupled to the set of acceptable commands, a comparison module for comparing the commands that access the database during an operational phase with the commands in the set of acceptable commands.

21. (Canceled)

22. (Currently Amended) The method of claim 1, ~~further comprising the step of establishing new categories responsive to the observed commands, and~~ wherein:

the statistical analysis further determines whether a predetermined frequency threshold for establishing the ~~new~~ categories has been exceeded; and

the training phase ends responsive to a determination that the predetermined frequency threshold has been exceeded.

23. (Canceled)

24. (Previously Presented) The method of claim 1, further comprising:

determining whether a predetermined period of time for the training phase has elapsed; and

ending the training phase responsive to a determination that the predetermined period of time has elapsed.

25. (New) The computer-readable storage medium of claim 20, wherein:

the statistical analysis further determines whether a predetermined frequency threshold for establishing the categories has been exceeded; and

the training phase ends responsive to a determination that the predetermined frequency threshold has been exceeded.

Allowable Subject Matter

5. Claims 1, 3, 4, 6-11, 13-16, 18-20, 22, 24, and 25 are allowed.

6. The following is an examiner's statement of reasons for allowance:

Independent Claims 1, 16, and 20 are directed to computer implemented methods for real time training of a database intrusion detection system or software implementations thereof. Each independent claim includes, during a training phase, observing commands accessing the database in real time, establishing categories based on the observed commands and grouping the commands into the established categories, and deriving a set of acceptable commands from the observed and grouped commands. Each independent claim further includes ending the training phase based on a determination that a predetermined threshold number of categories has been established. The closest cited prior art, Ramarao and Gruper, disclosed methods in which an intrusion detection system derives a set of acceptable commands and groups the commands into categories, such as by generalizing the commands into forms corresponding to the claimed "canonicalized" commands. The cited prior art further discloses systems having a real time learning mode in which commands are observed and where the training phase is ended responsive to a statistical analysis. Additional cited art, Yeager, discloses ending a training phase in response to reaching a threshold frequency of learning new patterns, i.e. categories, and Applicant admitted prior art further suggests that the principles of intrusion detection systems can be applied to detecting intrusions in databases. However, none of the cited prior art teaches or suggests, alone or in combination, that a threshold number of new categories is used as the condition for ending the real time training phase for an intrusion detection system. Therefore, the claims are allowable over the cited prior art.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ZAD/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437